1 Introduction

Much of the recent work on finite completely primary rings has demonstrated the fundamental importance of these rings in the structure theory of finite rings with identity. Let R be a finite ring. It turns out that R has a unique maximal ideal if and only if it is a full matrix ring over a completely primary ring. In particular, rings with a unique maximal ideal are not necessarily completely primary. Therefore, the study of rings with a unique maximal ideal (i.e. Local rings) reduces to the study of completely primary rings.

More evidence for the importance of completely primary rings comes from the fact that any commutative ring is a direct sum of completely primary rings. Moreover, any finite ring R is of the form $S + N$, where $S \cap N = \{0\}$ with N a subgroup of the Jacobson Radical of R and S a direct sum as an additive abelian group of certain matrix rings over completely primary rings (see [7]).

In this paper we consider rings of characteristic p with property(T) (see [1]). Clearly, such rings are completely primary. The rings of characteristics p^2 and p^3 with property(T) will be considered in later work.

In Section 2, we collect some preliminary results on finite completely primary rings. In Section 3, we give a construction of rings with property(T) and characteristic p, and in Section 4, we formulate the isomorphism problem of these rings. Section 5 considers the problem of enumerating certain cases of these rings.

2 Preliminaries

Let R be a finite ring. Then the following results will be assumed, and for details the reader is referred to [1], [4] and [9]:

2.1 Every element in R is either a zero-divisor or a unit, and there is no distinction between left and right zero-divisors (units).

2.2 If R is also completely primary with characteristic p^k and Jacobson radical M, then

(i) $|R| = p^{nr}$, for some positive integers n and r such that $k \leq n$;

(ii) $R/M \cong GF(p^r)$, the field of p^r elements;

(iii) If $k = n$, then $R = \mathbf{Z}_{p^k}[b]$, where b is an element of R of multiplicative order $p^r - 1$; $M = pR$ and $Aut(R) \cong Aut(R/pR)$.

The rings in 2.2(iii) shall be denoted by $GR(p^{nr}, p^n)$ and are called *Galois rings*.

2.3 If R is also completely primary with characteristic p^k and Jacobson radical M such that $|R/M| = p^r$, then R has a coefficient subring R_o of the form $GR(p^{kr}, p^k)$ which is clearly a maximal Galois subring of R. Furthermore, any two coefficient subrings are conjugate in R and there exist $m_1, \ldots, m_h \in M$ and $\sigma_1, \ldots, \sigma_h \in Aut(R_o)$ such that

(i) $R = R_o \bigoplus \sum_{i=1}^{h} \bigoplus R_i m_i$ (as R_o-modules);

(ii) $m_i r = r^{\sigma_i} m_i$, for every $r \in R_o$.

The σ_i are uniquely determined by R and R_o and are called the automorphisms associated with the m_i with respect to R_o.

3 Rings with property(T) and characteristic p

Let F be the Galois field $GF(p^r)$. For integers s, t, λ with $1 \leq t \leq s^2$, $\lambda \geq 0$, let U, V, W be s, λ, $t-$dimensional vector spaces over F, respectively. Since F is commutative, we can think of them as both left and right F-spaces. Let $\left(a_{ij}^k\right)$be t compatible matrices of size $s \times s$ with entries in F, $\{\sigma_1, \ldots, \sigma_s\}$, $\{\tau_1, \ldots, \tau_\lambda\}$, $\{\theta_1, \ldots, \theta_t\}$ be sets of automorphisms of F (with possible repetitions) and let $\{\sigma_i\}$ and $\{\theta_k\}$ satisfy the additional condition that if $a_{ij}^k \neq 0$, for any k with $1 \leq k \leq t$, then $\theta_k = \sigma_i \sigma_j$. Let R be the additive group direct sum

$$R = F \oplus U \oplus V \oplus W.$$

Then R may be given a ring structure via an appropriate multiplication (see e.g. [1]). The ring R is said to be given by Construction A, and the following results are proved in [1]:

Theorem 3.1 *The ring R given by Construction A is a ring with property(T) and of characteristic p. Conversely, every ring with property(T) and characteristic p is isomorphic to one given by Construction A.*

Theorem 3.2 *Let R be a ring of Construction A. Then the field F lies in the centre of R if and only if $\sigma_i = \tau_\mu = \theta_k = id_F$, for all $i = 1, \ldots, s$; $\mu = 1, \ldots, \lambda$; $k = 1, \ldots, t$; and R is commutative if and only if $a_{ij}^k = a_{ji}^k$, for all $i, j = 1, \ldots, s$.*

In what follows, the integers p, n, r, s, t, and λ, shall be called the invariants of R.

It is clear that what we have named invariants are indeed that, that is, isomorphic rings have that same invariants. On the other hand, it is easy to find examples of non-isomorphic rings with property(T) and characteristic p with the same invariants.

4 The isomorphism problem

In this section, we formulate the isomorphism problem of rings with property(T) and characteristic p. We know that all rings of this type are rings of Construction A. So, since $M^2 \subseteq ann(M)$, we can write

$$R = F \oplus U \oplus N, \text{ where } N = V \oplus W,$$

and if we define $v_1, \ldots, v_\lambda$ by $w_{t+1}, \ldots, w_{t+\lambda}$, and $\tau_1, \ldots, \tau_\lambda$ by $\theta_{t+1}, \ldots, \theta_{t+\lambda}$, respectively, then the multiplication in R becomes

$$(\alpha_o,\ \sum_i \alpha_i u_i,\ \sum_{k=1}^{t+\lambda} \gamma_k w_k) \cdot (\alpha_o',\ \sum_i \alpha_i' u_i,\ \sum_{k=1}^{t+\lambda} \gamma_k' w_k)$$

$$= (\alpha_o \alpha_o',\ \sum_i [\alpha_o \alpha_i' + \alpha_i (\alpha_o')^{\sigma_i}] u_i,\ \sum_k [\alpha_o \gamma_k' + \gamma_k (\alpha_o')^{\theta_k} + \sum_{i,j=1}^{s} a_{ij}^k \alpha_i (\alpha_j')^{\sigma_i}] w_k).$$

where $a_{ij}^k = 0$, for all $k = t + \lambda$, $\lambda \geq 1$.

Let R be the ring given by the above multiplication with respect to the compatible matrices (a_{ij}^k), with entries from F, and automorphisms $\sigma_i,\ \theta_k \in Aut(F)$ $(i = 1, \ldots, s;\ k = 1, \ldots, t + \lambda)$; with $\theta_k = \sigma_i \sigma_j$ for any k with $1 \leq k \leq t$, if $a_{ij}^k \neq 0$. Let $A = \{(a_{ij}^k) : k = 1, \ldots, t\}$, and let us denote the ring R with the above multiplication by $R(A, \sigma_i, \theta_k)$.

Thus, up to isomorphism, the ring $R(A, \sigma_i, \theta_k)$ is given by the t compatible matrices (a_{ij}^k) and the automorphisms $\sigma_i,\ \theta_k$, where σ_i and θ_k occur with multiplicity n_i and n_k, respectively $(i = 1, \ldots, s;\ k = t + 1, \ldots, t + \lambda)$.

Let now R' be another ring of the same type with the same invariants p, n, r, s, t, λ;

$$R' = F \oplus U' \oplus N', \text{ where } N' = V' \oplus W',$$

with respect to compatible matrices $D = \{(d_{ij}^k) : k = 1, \ldots, t\}$ and associated automorphisms $\sigma_i',\ \theta_k'$. Let σ_i' and θ_k' occur with multiplicity n_i' and n_k', respectively, and denote R' by $R(D, \sigma_i', \theta_k')$.

We assume that the rings $R(A, \sigma_i, \theta_k)$ and $R(D, \sigma_i', \theta_k')$ are constructed from a common maximal Galois subfield F.

We introduce the symbol M^σ to denote $\sigma((a_{ij}))$ if $M = (a_{ij})$.

Lemma 4.1 *With the above notations,*

$$R(A, \sigma_i, \theta_k) \cong R(D, \sigma_i', \theta_k')$$

if and only if there exist $B = (\beta_{\rho k}) \in GL(t, F)$, $C \in GL(s, F)$, $\sigma \in Aut(F)$ such that

$$D_\rho = \sum_{k=1}^{t} \beta_{k\rho} C^T A_k^\sigma C^{\sigma_\mu};$$

$\{\sigma_1, \ldots, \sigma_s\} = \{\sigma_1^{'}, \ldots, \sigma_s^{'}\}$, $\{\theta_{t+1}, \ldots, \theta_{t+\lambda}\} = \{\theta_{t+1}^{'}, \ldots, \theta_{t+\lambda}^{'}\}$ *and (after possible reindexing),* $n_i = n_i^{'}$, $n_k = n_k^{'}$ *for* $i = 1, \ldots, s;\ k = t+1, \ldots, t+\lambda$.

Proof Suppose there is an isomorphism

$$\phi : R(A, \sigma_i, \theta_k) \to R(D, \sigma_i^{'}, \theta_k^{'}).$$

Then, $\phi(F)$ is a maximal Galois subfield of $R(D, \sigma_i^{'}, \theta_k^{'})$ so there exits an invertible element $w \in R(D, \sigma_i^{'}, \theta_k^{'})$ such that $w\phi(F)w^{-1} = F$.

Now, consider the map

$$\psi : R(A, \sigma_i, \theta_k) \to R(D, \sigma_i^{'}, \theta_k^{'})$$

defined by

$$r \mapsto w\psi(r)w^{-1}.$$

Then, clearly, ψ is an isomorphism from $R(A, \sigma_i, \theta_k)$ to $R(D, \sigma_i^{'}, \theta_k^{'})$ which sends F to itself.

Also

$$\psi(0,\ \sum_i \alpha_i u_i,\ 0) = (0,\ \sum_\nu \sum_i \psi(\alpha_i)\alpha_{\nu i} u_\nu^{'},\ y^{'}) \quad (y^{'} \in N^{'});$$

and

$$\psi(0,\ 0,\ \sum_k \gamma_k w_k) = (0,\ 0,\ \sum_\rho \sum_k \psi(\gamma_k)\beta_{\rho k} w_\rho^{'}).$$

Therefore,

$$\psi(0,\ \sum_i \alpha_i u_i,\ 0) \cdot \psi(0,\ \sum_i \alpha_i^{'} u_i,\ 0)$$

$$= (0,\ \sum_\nu \sum_i \psi(\alpha_i)\alpha_{\nu i} u_\nu^{'},\ y^{'}) \cdot (0,\ \sum_\nu \sum_i \psi(\alpha_i^{'})\alpha_{\nu i} u_\nu^{'},\ y^{''})$$

$$= (0,\ 0,\ \sum_\rho \sum_{\nu,\mu=1}^{s} \sum_{i,j=1}^{s} \psi(\alpha_i)\psi(\alpha_j^{'})^{\sigma_\nu} \alpha_{\nu i} \alpha_{\mu j}^{\sigma_\nu} d_{\nu\mu}^{\rho} w_\rho^{'}).$$

On the other hand,

$$\psi((0,\ \sum_i \alpha_i u_i,\ 0) \cdot (0,\ \sum_i \alpha_i^{'} u_i,\ 0)) = \psi(0,\ 0,\ \sum_k \sum_{i,j=1}^{s} \alpha_i (\alpha_j^{'})^{\sigma_i} a_{ij}^k w_k)$$

$$= (0,\ 0,\ \sum_\rho \sum_{k=1}^{t} \sum_{i,j=1}^{s} \psi(\alpha_i (\alpha_j^{'})^{\sigma_i}) \beta_{\rho k} \psi(a_{ij}^k) w_\rho^{'}).$$

It follows that

$$\sum_{\nu,\mu=1}^{s}\sum_{i,j=1}^{s}\psi(\alpha_i)\psi(\alpha_j^{'})^{\sigma_\nu}\alpha_{\nu i}\alpha_{\mu j}^{\sigma_\nu}d_{\nu\mu}^{\rho}=\sum_{k=1}^{t}\sum_{i,j=1}^{s}\psi(\alpha_i(\alpha_j^{'})^{\sigma_i})\beta_{\rho k}\psi(a_{ij}^{k}). \qquad 4.1$$

Now, $\psi|_F$ is an automorphism of F, and therefore, $\psi(a_{ij}^k)=\sigma(a_{ij}^k)$, for some $\sigma\in Aut(F)$. Hence, $\sigma_\nu=\sigma_i$, for all $i,\nu=1,\ldots,s$. Hence, equation 4.1 now implies that

$$E^T D_\rho E^{\sigma_\mu}=\sum_{k=1}^{s}\beta_{k\rho}A_k^{\sigma},\ with\ E=(\alpha_{\mu j});$$

that is

$$D_\rho=C^T[\sum_{k=1}^{t}\beta_{k\rho}A_k^{\sigma}]C^{\sigma_\mu}=\sum_{k=1}^{t}\beta_{k\rho}C^TA_k^{\sigma}C^{\sigma_\mu},$$

where $C=E^{-1}$, as required.

That $\{\sigma_1,\ldots,\sigma_s\}=\{\sigma_1^{'},\ldots,\sigma_s^{'}\}$, $\{\theta_{t+1},\ldots,\theta_{t+\lambda}\}=\{\theta_{t+1}^{'},\ldots,\theta_{t+\lambda}^{'}\}$ and (after possible reindexing), $n_i=n_i^{'}$, $n_k=n_k^{'}$ for $i=1,\ldots,s;\ k=t+1,\ldots,t+\lambda$; follows from the fact that $R(A,\sigma_i,\theta_k)$ and $R(D,\sigma_i^{'},\theta_k^{'})$ are constructed from a common maximal Galois subfield F.

Now, suppose that there exist $B=(\beta_{\rho k})\in GL(t,F)$, $C\in GL(s,F)$, $\sigma\in Aut(F)$ such that

$$D_\rho=\sum_{k=1}^{t}\beta_{k\rho}C^TA_k^{\sigma}C^{\sigma_\mu};$$

with $\{\sigma_1,\ldots,\sigma_s\}=\{\sigma_1^{'},\ldots,\sigma_s^{'}\}$, $\{\theta_{t+1},\ldots,\theta_{t+\lambda}\}=\{\theta_{t+1}^{'},\ldots,\theta_{t+\lambda}^{'}\}$ and (after possible reindexing), $n_i=n_i^{'}$, $n_k=n_k^{'}$ for $i=1,\ldots,s;\ k=t+1,\ldots,t+\lambda$.

Consider the map

$$\psi: R(A,\sigma_i,\theta_k)\rightarrow R(D,\sigma_i^{'},\theta_k^{'})$$

given by

$$(\alpha_o,\ \sum_i\alpha_iu_i,\ \sum_k\gamma_kw_k)\mapsto(\alpha_o^{\sigma},\ \sum_\nu\sum_i\alpha_i^{\sigma}\alpha_{\nu i}u_\nu^{'},\ \sum_\rho\sum_k\gamma_k^{\sigma}\beta_{k\rho}w_\rho^{'}).$$

Then, it is easy to verify that ψ is an isomorphism of the ring $R(A,\sigma_i,\theta_k)$ onto the ring $R(D,\sigma_i^{'},\theta_k^{'})$.

Corollary 4.2 *Let A and D be sets of compatible matrices with entries from F. If A and D generate the same vector space over F,and if $\sigma_i=\sigma_i^{'}$, $\theta_k=\theta_k^{'}$ with $n_i=n_i^{'}$, $n_k=n_k^{'}$, then*

$$R(A,\sigma_i,\theta_k)\cong R(D,\sigma_i^{'},\theta_k^{'}).$$

5 The Enumeration problem

In this section, we consider the problem of finding the number of distinct (up to isomorphism) types of rings with property(T) and characteristic p. We find those rings of Construction A which give rise to distinct non-isomorphic rings.

We consider this for certain cases.

5.1 The case where $s = 1$

For this case, R is a ring of Construction A with $t = 1$, $\lambda \geq 0$. Then, the only parameters in the definition of R are the automorphisms σ_1, θ_k, $(k = 1+\lambda,\ \lambda \geq 0)$, $\theta_1 = \sigma_1^2$; and the element $a_{11}^1 \in F^*$.

Let us denote the ring R by $R(a_{11}^1, \sigma_1, \theta_k)$. Thus, up to isomorphism, the ring $R(a_{11}^1, \sigma_1, \theta_k)$ is given by the element $a_{11}^1 \in F^*$ and the automorphisms σ_1, θ_k, where for θ_k, $k > 1$, θ_k occurs with multiplicity n_k.

If $R(d_{11}^1, \sigma_1^{'}, \theta_k^{'})$ is another ring of the same type with the same invariants p, n, r, s, t, λ, with $s = t = 1$, then by Lemma 4.1

$$R(a_{11}^1, \sigma_1, \theta_k) \cong R(d_{11}^1, \sigma_1^{'}, \theta_k^{'})$$

if and only if there exist $\beta_{11},\ \gamma \in F^*$ and $\theta \in Aut(F)$ such that

$$d_{11}^1 = \gamma\gamma^{\sigma_1}\beta_{11}(a_{11}^1)^{\theta};\ \sigma_1 = \sigma_1^{'},\ \{\theta_2, \ldots, \theta_{1+\lambda}\} = \{\theta_1^{'}, \ldots, \theta_{1+\lambda}^{'}\}$$

and (after possible reindexing) $n_k = n_k^{'}$, for every $k = 2, \ldots, 1 + \lambda$.

As a result of Lemma 4.1, if $\gamma,\ \beta_{11} \in F^*$, then the rings $R(a_{11}^1, \sigma_1, \theta_k)$ and $R(\gamma\gamma^{\sigma_1}\beta_{11}(a_{11}^1)^{\theta}, \sigma_1, \theta_k)$ are isomorphic. Hence, we can select $\gamma = 1$ and $\beta_{11} = ((a_{11}^1)^{\theta})^{-1}$ to see that the rings $R(a_{11}^1, \sigma_1, \theta_k)$ and $R(1, \sigma_1, \theta_k)$ are isomorphic. So, counting the isomorphism classes of the rings $R(a_{11}^1, \sigma_1, \theta_k)$ is a question of counting the number of distinct ways of selecting the automorphisms.

Consider now the automorphisms $\sigma_1,\ \theta_2, \ldots, \theta_{1+\lambda}$. Since $|Aut(F)| = r$, the number of ways in which we can select σ_1 from $Aut(F)$ is r. Also, the number of ways we can select $\theta_2, \ldots, \theta_{1+\lambda}$ from $Aut(F)$ (θ_k not necessarily distinct), is the number of solutions in the equation

$$x_1 + x_2 + \ldots + x_r = \lambda$$

in non-negative integers $x_1,\ x_2, \ldots, x_r \in \{0, 1, \ldots, \lambda\}$. This is well known to be (see [6], page 2)

$$\begin{pmatrix} r + \lambda - 1 \\ \lambda \end{pmatrix}.$$

Therefore, for a fixed $a_{11}^1 \in F^*$, a $\sigma_1 \in Aut(F)$ and a λ-selection of $\theta \in Aut(F)$, there is only one ring up to isomorphism. Therefore, the number of isomorphism classes of rings of Construction A of the same characteristic p and same order, with the same invariants p, n, r, s, t, λ, where $s = t = 1$, is

$$r \cdot \begin{pmatrix} r + \lambda - 1 \\ \lambda \end{pmatrix}.$$

We have thus proved the following

Lemma 5.1 *The number of mutually non-isomorphic rings with property(T) and characteristic p and of the same order with the same invariants p, n, r, s, t, λ, in which $s = t = 1$, is*

$$r \cdot \begin{pmatrix} r + \lambda - 1 \\ \lambda \end{pmatrix}.$$

Of these, only one is commutative, the others are not.

If, in particular, $\lambda = 0$, then the rings are principal ideal rings, so that we have

Corollary 5.2 *The number of mutually non-isomorphic principal ideal rings with property(T) and characteristic p (and of the same order) with the same invariants p, n, r is r. Further, only one is commutative, the others are not.*

5.2 The case where $t = s^2$

Let R be a ring of Construction A with the invariants p, n, r, s, t, λ, where $t = s^2$; and let σ_i, θ_k $(i = 1, \ldots, s;\ k = 1, \ldots, t, t+1, \ldots, t+\lambda)$ be the associated automorphisms of R with respect to a fixed maximal Galois subfield F of R, and let $A_1, A_2, \ldots, A_t$ be the compatible structural matrices of R. Let $\mathcal{A}$ denote the subspace of $M_s(F)$ generated by the matrices $A_1, \ldots, A_t$ over F. Since $t = s^2$, $\mathcal{A} = M_s(F)$.

Let now R' be another ring of the same type with the same invariants p, n, r, s, t, λ, where $t = s^2$, with respect to the automorphisms $\sigma_j^{'}, \theta_l^{'} \in Aut(F)$ $(j = 1, \ldots, s;\ l = 1, \ldots, t, t+1, \ldots, t+\lambda)$ and compatible structural matrices $D_1, \ldots, D_t$, with respect to a common fixed maximal Galois field F. Let $\mathcal{D}$ denote the subspace of $M_s(F)$ generated by $D_1, \ldots, D_t$ over F. As before, since $t = s^2$, then $\mathcal{D} = M_s(F)$.

But $\mathcal{A} = \mathcal{D} = M_s(F)$. Thus, up to isomorphism, the rings R and R' are determined by the automorphisms σ_i, θ_k and σ_j', θ_l' $(i, j = 1, \ldots, s;\ k, l = t + 1, \ldots, t + \lambda)$, respectively.

Lemma 5.3 *The number of mutually non-isomorphic rings with property(T) and characteristic p, with the same invariants p, n, r, s, t, λ, where $t = s^2$ is*

$$\binom{r+s-1}{s} \cdot \binom{r+\lambda-1}{\lambda}.$$

All of these rings are non-commutative.

Proof From the above discussion, it is clear that the number of isomorphism classes in question is the number of ways in which we can select $\{\sigma_1, \ldots, \sigma_s\}$ and $\{\theta_{t+1}, \ldots, \theta_{t+\lambda}\}$ $(\sigma_i, \theta_k$ not necessarily distinct) from $Aut(F)$. Since $|Aut(F)| = r$, the number in question is the number of solutions of the two equations

$$x_1 + x_2 + \ldots + x_r = s,$$

and

$$y_1 + y_2 + \ldots + y_r = \lambda$$

in non-negative integers $x_1, \ldots, x_r \in \{0, 1, \ldots, s\}$ and $y_1, \ldots, y_r \in \{0, 1, \ldots, \lambda\}$. This is well known to be

$$\binom{r+s-1}{s} \cdot \binom{r+\lambda-1}{\lambda}.$$

5.3 The case where F lies in the centre of R

We now consider the case where the maximal Galois subfield F lies in the centre of R, that is, the case where all the associated automorphisms of R are equal to the identity automorphism (Theorem 3.2).

We note that the description of the rings of this type reduces to the case where $ann(M)$ coincides with M^2. Therefore, to enumerate the rings of this type of a given order, say p^{nr}, where $ann(M)$ does not coincide with M^2, we shall first write all the rings of this type of order $\leq p^{nr}$, where $ann(M)$ coincides with M^2.

In what follows, we assume that $ann(M) = M^2$.

5.3.1 The case with $t = 1$

Suppose now that R is a ring with property(T) and characteristic p with the invariants p, n, r, s, t; where $t = 1$. Then, the ring R is defined by one structural matrix A_1, where A_1 is a non-zero $s \times s$ compatible matrix with entries from F.

Now, let $R(D_1)$ be another ring with property(T) and characteristic p with the same invariants p, n, r, s, t, where $t = 1$, and of the same order as $R(A_1)$ and assume that they are constructed from a common maximal Galois subfield F. Then, by Lemma 4.1, $R(A_1) \cong R(D_1)$ if and only if there exists a $\sigma \in Aut(F)$, an invertible matrix $C \in M_s(F)$ and a non-zero element $\beta \in F$ such that

$$D_1 = \beta^{-1} C^T A_1^\sigma C.$$

Congruence of matrices in the classical sense implies equivalence in the sense defined above but not vice-versa as the following example shows:

Example Let $F = \mathbf{F}_4 = \{0, 1, \alpha, 1 + \alpha\}$ and $\sigma \in Aut(F)$ such that $\sigma : x \mapsto x^2$, for every $x \in F$. Consider the matrices

$$\begin{pmatrix} 1 & 0 \\ \alpha & 1 \end{pmatrix}, \qquad \begin{pmatrix} 1 & 0 \\ 1+\alpha & 1 \end{pmatrix} \in M_2(F).$$

The F-spaces generated by these two matrices are equivalent since, for instance,

$$\begin{pmatrix} 1 & 0 \\ \alpha & 1 \end{pmatrix}^\sigma = \begin{pmatrix} 1 & 0 \\ 1+\alpha & 1 \end{pmatrix};$$

while the two matrices are not congruent.

However, in the cases where the automorphisms σ can be reduced to the identity (for instance, if R is commutative or if F is a prime field) then equivalence comes very close to congruence (the element β makes the only difference). So, it makes sense to look at congruence classes.

Let $N(s)$ denote the number of congruence classes of $s \times s$ matrices over $F \cong GF(p^r)$. In [10], Waterhouse implicitly computed the number of congruence classes of $n \times n$ matrices over finite fields, and in [8], Newman obtained the number and representatives of congruence classes of $n \times n$ symmetric matrices of positive rank $\leq n$ over finite fields, and we restate these results here in our notation for easy reference.

Theorem 5.4 *$N(s)$ is the coefficient of t^s in*

$$\prod_{k \geq 1} (1 + t^k)^e (1 - qt^{2k})^{-1} (1 - t^k)^{-1},$$

where $e = 1$ for even q and $e = 2$ for odd q.

Theorem 5.5 *(i) Let F be a finite field of characteristic 2. Then every symmetric matrix of $M_n(F)$ of rank r is congruent to $I_r \oplus 0$ (r odd), or to $I_r \oplus 0$ or $(r/2)T \oplus 0$ (r even), where kT denotes the direct sum of k copies of*

$$T = \begin{pmatrix} 0 & 1 \\ 1 & 0 \end{pmatrix};$$

and these are not congruent.

(ii) Let F be a finite field of characteristic different from 2. Then, every symmetric matrix of $M_n(F)$ of rank r is congruent to $I_r \oplus 0$ or to $gI_1 \oplus I_{r-1} \oplus 0$, where g is a fixed non-square in F; these are not congruent. Thus, the symmetric matrices of any given rank fall into precisely two congruence classes.

We now consider the problem of finding the number of isomorphism classes of rings with property(T) and characteristic p with same invariants p, n, r, s, t, λ; where $s > 1$ and $t = 1$. The solution of this problem depends on the much more difficult classical problem of the classification of bilinear forms over finite fields.

Consider the matrices $\beta^{-1}C^TAC$, where $A \in M_s(F_q)$.

Case 1. Suppose that $s = 2$ and $t = 1$. In [2], Bremser obtained the congruence classes of matrices in $GL_2(F_q)$, and showed that there are $q+3$ for odd q and $q+1$ for even q. The number of congruence classes in $M_2(F)$ over a finite field F of any characteristic p can be calculated from the formula in Theorem 5.4 (see also Waterhouse [10]), and here we give a complete set of representatives of these classes, which include those obtained by Bremser in [2].

(i) $Char F \neq 2$.

$$\begin{pmatrix} 0 & 0 \\ 0 & 0 \end{pmatrix}, \quad \begin{pmatrix} 0 & 1 \\ -1 & 0 \end{pmatrix}, \quad \begin{pmatrix} 1 & 0 \\ 0 & 0 \end{pmatrix}, \quad \begin{pmatrix} 1 & 0 \\ 1 & 0 \end{pmatrix},$$

$$\begin{pmatrix} g & 0 \\ 0 & 0 \end{pmatrix}, \quad \begin{pmatrix} g & 0 \\ 2g & g \end{pmatrix}, \quad \begin{pmatrix} 1 & 0 \\ 0 & 1 \end{pmatrix}, \quad \begin{pmatrix} 1 & 0 \\ 0 & g \end{pmatrix},$$

$$\begin{pmatrix} 1 & 0 \\ \gamma & 1 \end{pmatrix}, \quad \begin{pmatrix} 1 & 0 \\ \gamma & g \end{pmatrix},$$

where γ runs over a complete set of coset representatives of $\{\pm 1\}$ in F^*; these are $q+7$ altogether.

(ii) $Char F = 2$.

$$\begin{pmatrix} 0 & 0 \\ 0 & 0 \end{pmatrix}, \quad \begin{pmatrix} 1 & 0 \\ 0 & 0 \end{pmatrix}, \quad \begin{pmatrix} 1 & 0 \\ 0 & 1 \end{pmatrix}, \quad \begin{pmatrix} 0 & 1 \\ 1 & 0 \end{pmatrix},$$

$$\begin{pmatrix} 1 & 0 \\ 1 & 0 \end{pmatrix}, \quad \begin{pmatrix} 1 & 0 \\ \alpha & 1 \end{pmatrix}, \quad \alpha \in F^*$$

and these are $q+4$ in all.

Now, suppose $|F| = 2$. Then the non-zero congruence classes are

$$\begin{pmatrix} 1 & 0 \\ 0 & 0 \end{pmatrix}, \quad \begin{pmatrix} 1 & 0 \\ 0 & 1 \end{pmatrix}, \quad \begin{pmatrix} 0 & 1 \\ 1 & 0 \end{pmatrix},$$

$$\begin{pmatrix} 1 & 0 \\ 1 & 0 \end{pmatrix}, \quad \begin{pmatrix} 1 & 0 \\ 1 & 1 \end{pmatrix}.$$

Since $\beta = 1$ in this case, these matrices also represent equivalence classes. Notice also that the equivalence class

$$\begin{pmatrix} 1 & 0 \\ 0 & 0 \end{pmatrix} \text{ contains the compatible matrix } \begin{pmatrix} 1 & 1 \\ 1 & 1 \end{pmatrix};$$

and therefore, we include this class among the equivalence classes that correspond to rings with property(T). Hence, the number of mutually non-isomorphic rings of this type is 5, which is the number of non-zero congruence classes.

Suppose $|F| = p$, $p \neq 2$, then it can be deduced from the class representatives above that the number of non-zero congruence classes is $p+6$. Now, if $\beta = g$ is an element of $\mathbf{F}_p^*$, it is easy to see that the congruence class

$$\begin{pmatrix} g & 0 \\ 2g & g \end{pmatrix} \text{ is equivalent to one of the classes of the form } \begin{pmatrix} 1 & 0 \\ \gamma & 1 \end{pmatrix}$$

in (i) above. Also, the classes

$$\begin{pmatrix} 1 & 0 \\ 0 & 0 \end{pmatrix} \text{ and } \begin{pmatrix} g & 0 \\ 0 & 0 \end{pmatrix}$$

are equivalent. Moreover, all the equivalence classes contain at least one compatible matrix. Therefore, the number of equivalence classes in this case is $p+4$ and this also gives the number and models for the corresponding rings.

Case 2. Suppose $s = 3$ and $t = 1$. In [5], B. Corbas and G. D. Williams have obtained the matrix representatives for bilinear forms on a three dimensional vector space over a finite field of any characteristic, without assuming that the form is symmetric or non-degenerate. We give here a full list of the congruence classes as given in their main Theorem.

(i) $Char F \neq 2$.

$$\begin{pmatrix} 0 & 0 & 0 \\ 0 & 0 & 0 \\ 0 & 0 & 0 \end{pmatrix}, \begin{pmatrix} 1 & 0 & 0 \\ 0 & 0 & 0 \\ 0 & 0 & 0 \end{pmatrix}, \begin{pmatrix} \varepsilon & 0 & 0 \\ 0 & 0 & 0 \\ 0 & 0 & 0 \end{pmatrix}, \begin{pmatrix} 1 & 0 & 0 \\ 0 & 1 & 0 \\ 0 & 0 & 0 \end{pmatrix},$$

$$\begin{pmatrix} 1 & 0 & 0 \\ 0 & \varepsilon & 0 \\ 0 & 0 & 0 \end{pmatrix}, \begin{pmatrix} 1 & 0 & 0 \\ 0 & 1 & 0 \\ 0 & 0 & 1 \end{pmatrix}, \begin{pmatrix} 1 & 0 & 0 \\ 0 & 1 & 0 \\ 0 & 0 & \varepsilon \end{pmatrix}, \begin{pmatrix} \mu & 0 & 0 \\ 0 & 0 & 1 \\ 0 & -1 & 0 \end{pmatrix},$$

$$\begin{pmatrix} \mu & 0 & 0 \\ 0 & 0 & 0 \\ 0 & 1 & 0 \end{pmatrix}, \begin{pmatrix} \mu & 0 & 0 \\ 0 & \varepsilon & 0 \\ 0 & 2\varepsilon & \varepsilon \end{pmatrix}, \begin{pmatrix} \mu & 0 & 0 \\ 0 & 1 & 0 \\ 0 & \gamma & 1 \end{pmatrix}, \begin{pmatrix} \mu & 0 & 0 \\ 0 & 1 & 0 \\ 0 & \gamma & \varepsilon \end{pmatrix},$$

$$\begin{pmatrix} \mu & 0 & 0 \\ 0 & 0 & 1 \\ 1 & 1 & 0 \end{pmatrix},$$

where $\mu \in \{0,\ 1,\ \varepsilon\}$, with ε an arbitrary but fixed non-square in F^*, and γ runs over a complete set of coset representatives of $\{1,\ -1\}$ in F^*. Their total number is $3q + 16$.

(ii) $Char F = 2$.

$$\begin{pmatrix} 0 & 0 & 0 \\ 0 & 0 & 0 \\ 0 & 0 & 0 \end{pmatrix}, \begin{pmatrix} 1 & 0 & 0 \\ 0 & 0 & 0 \\ 0 & 0 & 0 \end{pmatrix}, \begin{pmatrix} 1 & 0 & 0 \\ 0 & 1 & 0 \\ 0 & 0 & 0 \end{pmatrix}, \begin{pmatrix} 1 & 0 & 0 \\ 0 & 1 & 0 \\ 0 & 0 & 1 \end{pmatrix},$$

$$\begin{pmatrix} 0 & 0 & 0 \\ 0 & 0 & 1 \\ 0 & 1 & 0 \end{pmatrix}, \begin{pmatrix} \mu & 0 & 0 \\ 0 & 0 & 0 \\ 0 & 1 & 0 \end{pmatrix}, \begin{pmatrix} \mu & 0 & 0 \\ 0 & 1 & 0 \\ 0 & \gamma & 1 \end{pmatrix}, \begin{pmatrix} 1 & 0 & 0 \\ 0 & 0 & 0 \\ 1 & 1 & 0 \end{pmatrix},$$

$$\begin{pmatrix} 1 & 0 & 0 \\ 0 & 0 & 1 \\ 1 & 1 & 0 \end{pmatrix}, \begin{pmatrix} 1 & 0 & 0 \\ 0 & 0 & 1 \\ \alpha & 1 & 1 \end{pmatrix},$$

where $\mu \in \{0,\ 1\}$, $\gamma \in F^*$ and $X^2 + \alpha X + 1$ is an arbitrary but fixed irreducible polynomial of degree two over F. Their total number is $2q + 8$.

Now, suppose $|F| = 2$, then it can be deduced from the list of class representatives in (ii) above that the number of non-zero congruence classes is 11. Since in this case $\beta = 1$, these classes also represent the equivalence classes of 1-dimensional spaces of bilinear forms over $\mathbf{F}_2$. Further, since all the equivalence classes contain at least one compatible matrix, we conclude that the number of non-isomorphic rings with property(T) and characteristic 2 with same invariants and with maximal Galois subfield $\mathbf{F}_2$ is 11. The models of each of these is given by the corresponding equivalence class.

Now, suppose $|F| = p$, $p \neq 2$. Then the list of class representatives in (i) above gives $3p+15$ non-zero congruence classes. As β runs over the elements of $\mathbf{F}_p^*$, the congruence classes

$$\begin{pmatrix} \varepsilon & 0 & 0 \\ 0 & 0 & 0 \\ 0 & 0 & 0 \end{pmatrix}, \begin{pmatrix} 1 & 0 & 0 \\ 0 & 1 & 0 \\ 0 & 0 & \varepsilon \end{pmatrix}, \begin{pmatrix} 0 & 0 & 0 \\ 0 & \varepsilon & 0 \\ 0 & 2\varepsilon & \varepsilon \end{pmatrix}, \begin{pmatrix} 1 & 0 & 0 \\ 0 & \varepsilon & 0 \\ 0 & 2\varepsilon & \varepsilon \end{pmatrix},$$

and

$$\begin{pmatrix} \varepsilon & 0 & 0 \\ 0 & \varepsilon & 0 \\ 0 & 2\varepsilon & \varepsilon \end{pmatrix}, \text{ become equivalent to } \begin{pmatrix} 1 & 0 & 0 \\ 0 & 0 & 0 \\ 0 & 0 & 0 \end{pmatrix}, \begin{pmatrix} 1 & 0 & 0 \\ 0 & 1 & 0 \\ 0 & 0 & 1 \end{pmatrix},$$

$$\begin{pmatrix} 0 & 0 & 0 \\ 0 & 1 & 0 \\ 0 & \gamma & 1 \end{pmatrix}, \begin{pmatrix} \varepsilon & 0 & 0 \\ 0 & 1 & 0 \\ 0 & \gamma & 1 \end{pmatrix}, \text{ and } \begin{pmatrix} 1 & 0 & 0 \\ 0 & 1 & 0 \\ 0 & \gamma & 1 \end{pmatrix},$$

respectively. Furthermore, it is easy to show that all the congruence classes contain at least one compatible matrix, hence, all the equivalence classes contain at least one compatible matrix. Thus, the number of equivalence classes over $\mathbf{F}_p$, $p \neq 2$ is $3p + 10$.

In view of the above discussion, we may now state the following:

Proposition 5.6 *Let $N(s,\ 1)$ denote the total number of non-isomorphic rings with property(T) and characteristic p with maximal Galois subfield $\mathbf{F}_p$; and with the same invariants p, n, s, t, λ, where $t = 1$. Then,*
$N(2,\ 1) = 5$ or $p + 4$ according as $p = 2$ or otherwise;
$N(3,\ 1) = 11$ or $3p + 10$ according as $p = 2$ or $p \neq 2$.
In general, $N(s,\ 1) \leq N(s) - 1$, where $N(s)$ is as in Theorem 5.4. Moreover, this bound is reached when $p = 2$.

We next consider the matrices $\beta^{-1}C^TAC$, where $A \in \mathbf{M}_s(F)$ is symmetric and F is any finite Galois field $GF(p^r)$. Theorem 5.5 gives the number and representatives of congruence classes of $s \times s$ symmetric matrices of any positive rank $r \leq s$. Now, if $p \neq 2$, for any $s > 1$, the number of non-zero congruence classes is $2s$. It is easy to verify that each of these classes contains a compatible matrix. Also, as β runs over all the elements of F^*, we see that all the classes of odd rank reduce to one equivalence class, namely, to the class with 1's in the main diagonal, while those of even rank remain distinct. For instance,

$$\begin{pmatrix} 1 & 0 & 0 \\ 0 & 0 & 0 \\ 0 & 0 & 0 \end{pmatrix} \text{ and } \begin{pmatrix} \epsilon & 0 & 0 \\ 0 & 0 & 0 \\ 0 & 0 & 0 \end{pmatrix}$$

become equivalent to each other. Therefore, the number of equivalence classes of 1-dimensional symmetric bilinear forms over F when $p \neq 2$ is $\frac{3s-1}{2}$ if s is odd and $\frac{3s}{2}$ if s is even.

Now, if $p = 2$, the number of non-zero congruence classes of $s \times s$ symmetric matrices over F is $\frac{3s-1}{2}$ when s is odd; and $\frac{3s}{2}$ when s is even. Clearly, as β runs over all the elements of F^*, these congruence classes remain distinct equivalence classes. Furthermore, it is easy to see that each equivalence class contains a compatible matrix; hence, the above numbers give the number of non-isomorphic commutative rings with characteristic p and of the same invariants. The models of these can be deduced from Theorem 5.5.

We may then state the following:

Proposition 5.7 *Let $N_c(s,\ 1)$ denote the total number of isomorphism classes of commutative rings with property(T) and characteristic p with maximal Galois subfield $GF(p^r)$; and with the same invariants p, n, r, s, t, λ, where $t = 1$. Then*

$$N_c(s,\ 1) = \begin{cases} \frac{3s-1}{2} & if\ s\ is\ odd, \\ \frac{3s}{2} & if\ s\ is\ even, \end{cases}$$

for any prime p.

In the case where the rings are not commutative and the field F is not a prime field, it is intuitively obvious that, in general, there will be a lot fewer equivalence classes than congruence classes. Therefore, all we can say is that the number of isomorphism classes of the rings in question does not exceed $N(s)-1$; the number of non-zero congruence classes.

The study of how the congruence classes are subdivided into equivalence classes is obviously very important and we consider this in subsequent works.

5.3.2 The case with $s = 2$, $t = 2$

Let R be a ring with property(T) and characteristic p in which the maximal Galois subfield F lies in the centre and with invariants p, n, r, s, t, λ, where $s = 2$ and $t = 2$. Then, the ring R is defined by two structural matrices A_1 and A_2, where A_1 and A_2 are 2×2 compatible matrices over F. We know from Lemma 4.1 how two rings of the same type can be isomorphic with each other. Moreover, two rings of the same type are isomorphic if and only if their corresponding spaces of bilinear forms are equivalent.

Let $N(2,\ 2)$ denote the number of equivalence classes of 2-dimensional spaces of 2×2 matrices over F corresponding to 2-dimensional spaces of bilinear forms. The number of such equivalence classes may be determined and the class representatives may be obtained for particular values of p by using programs we devised that make use of elements from MATLAB. Here we give a representative of such programs in the Appendix. The number of equivalence classes $N(2,\ 2)$ is then given by the following:

$$N(2,\ 2) = \begin{cases} 10 & \text{if } |F| = 2 \\ 14 & \text{if } |F| = 3 \\ 20 & \text{if } |F| = 5 \\ 26 & \text{if } |F| = 7. \end{cases}$$

With these results, we may then state the following:

Proposition 5.8 *The number of mutually non-isomorphic rings with property(T) and characteristic p and of the same order with maximal Galois subfield $\mathbf{F}_p$, and with the same invariants $p,\ n,\ s,\ t,\ \lambda$, where $s = 2$ and $t = 2$, is*

$$\begin{cases} 10 & \text{if } p = 2, \\ 3p + 5 & \text{if } p \neq 2. \end{cases}$$

Of these, only 3 are commutative (for every prime p), the others are not.

5.3.3 The case with $s = 2$, $t = 3$

We now consider the problem of classifying all the rings of a given order with property(T) and characteristic p, in which the maximal Galois subfield F lies in the centre, for given invariants $p,\ r,\ n,\ s,\ t,\ \lambda$, where $s = 2$ and $t = 3$.

Let R be one such ring. Then, the ring R is defined by three 2×2 compatible structural matrices A_1, A_2 and A_3 over F. Then on the basis of Lemma 4.1, if $R(D)$ is isomorphic to $R(A)$, where $A = \{A_1,\ A_2,\ A_3\}$ and $D = \{D_1,\ D_2,\ D_3\}$, there exist matrices C in $GL(2,\ F)$ and $B = (\beta_{k\rho})$ in $GL(3,\ F)$ such that

$$\begin{aligned} D_1 &= \beta_{11}C^T A_1 C + \beta_{12}C^T A_2 C + \beta_{13}C^T A_3 C, \\ D_2 &= \beta_{21}C^T A_1 C + \beta_{22}C^T A_2 C + \beta_{23}C^T A_3 C, \\ D_3 &= \beta_{31}C^T A_1 C + \beta_{32}C^T A_2 C + \beta_{33}C^T A_3 C. \end{aligned}$$

Let $N(2,\ 3)$ denote the number of equivalence classes of 3-dimensional spaces of 2×2 matrices over F corresponding to 3-dimensional spaces of bilinear forms. Then, by the MATLAB program in the Appendix, we have

$$N(2,\ 3) = \begin{cases} 5 & \text{if } |F| = 2 \\ 7 & \text{if } |F| = 3 \\ 9 & \text{if } |F| = 5 \end{cases}$$

We have partial results to this problem, and conjecture the number of mutually non-isomorphic rings of order p^{nr} with property(T) and characteristic p.

Conjecture A *The number of mutually non-isomorphic rings with property(T) and characteristic p and of order p^{nr}, with maximal Galois subfield $\mathbf{F}_p$, and with the same invariants p, n, s, t, λ, where $s = 2$, $t = 3$, is*

$$\begin{cases} 5 & \text{if } p = 2, \\ p + 4 & \text{if } p \neq 2. \end{cases}$$

Of these, only one is commutative (for every prime p), the others are not.

It must be noted that the case $p = 2$ follows from the MATLAB program.

5.3.4 The case with $s = 3$, $t = 2$

By a program similar to that in the Appendix devised using elements from MATLAB, we find that the number of equivalence classes of 2-dimensional spaces of 3×3 matrices over $\mathbf{F}_2$ corresponding to 2-dimensional spaces of bilinear forms on 3 variables is 322. All these classes contain at least one compatible matrix, and therefore, we conclude that all these classes are representatives for the rings in question.

The number of mutually non-isomorphic rings of characteristic 2 with property(T) may now be given by the following result.

Proposition 5.9 *The number of mutually non-isomorphic rings with property(T) and characteristic $p = 2$ with maximal Galois subfield $\mathbf{F}_2$, and with the same invariants p, n, s, t, λ, where $s = 3$, $t = 2$; is* 322.

Of these, 14 *are commutative, the others are not.*

In the case where the field F is not prime, it is obvious that there will be more equivalence classes than we have in the case of prime subfields. Therefore, all we can say is that the number of isomorphism classes of rings with property(T) and characteristic p in which the maximal Galois subring F lies in the centre and with same invariants p, n, r, s, t, λ, with $s > 1$, does not exceed the number of distinct subspaces of $\mathbf{M}_s(F)$ of dimension t. This upper bound is reached in the case where $t = s^2$, since in this case, by Lemma 5.3, we only have one ring for any $s > 1$.

Acknowledgements

The author would like to thank Prof. D. Theo for many comments and illuminating discussions and Prof. B. Choudhary for comments on an earlier draft of this work.

References

[1] **C. J. Chikunji**, On a Class of Finite Rings; Communications in Algebra (*to appear, Fall 1999*).
[2] **P. S. Bremser**, Congruence Classes of Matrices in $GL_2(F_q)$, Discrete Math. 118 (1993), p243 - 249.
[3] **W. E. Clark**, A coefficient ring for finite non-commutative rings, Proc. Amer. Math. Soc. 33, No.1 (1972), p25 - 28.
[4] **B. Corbas**, Rings with few zero divisors, Math. Ann. 181 (1969), p1 - 7.
[5] **B. Corbas & G. D. Williams**, Matrix Representations for Three Dimensional Billinear Forms over Finite Fields, Discrete Mathematics 185 (1998) p51 - 61.
[6] **M. Hall, JR.**, Combinatorial Theory, Wiley (1986).
[7] **N. Jacobson**, Structure of rings, Amer. Math. Soc. Colloq. Publ. XXXVII (1964).
[8] **M. Newman**, Integral Matrices, Academic Press, N.Y. (1972).
[9] **R. Raghavendran**, Finite Associative Rings, Compositio Math. 21, Fasc. 2 (1969), p195 - 229.
[10] **W. C. Waterhouse**, The number of Congruence Classes in $M_n(F_q)$, Finite Fields and their Applications, 1 (1995), p57 - 63.

Appendix

A MATLAB Program for $s = 2$, $t = 3$ over F_3

```
function jo(a)
global A
global B
global C
T=[ ];
for i=1:12
  if a >= 2*3^(12 - i)  T(i) = 2;  a = a - 2*3^(12 - i);
   elseif a >= 3^(12 - i)  T(i) = 1; a = a - 3^(12 - i);
   else T(i) = 0;
  end
end
A = [T(1:2); T(3:4)];
B = [T(5:6); T(7:8)];
C = [T(9:10); T(11:12)];

function joh(a)
global M
T = [ ];
for i = 1:4
  if a >= 2*3^(4 - i)   T(i) = 2; a = a - 2*3^(4 - i);
    elseif a >= 3^(4 - i)  T(i) = 1;  a = a - 3^(4 - i);
     else  T(i) = 0;
   end
end
M = [T(1:2); T(3:4)];

function john(a)
global N
T = [ ];
for i = 1:9
  if a >= 2*3^(9 - i)   T(i) = 2;  a = a - 2*3^(9 - i);
   elseif  a >= 3^(9 - i)  T(i) = 1;  a = a - 3^(9 - i);
   else  T(i) = 0;
  end
end
N = [T(1:3); T(4:6); T(7:9)];

function ph(A, B, C)
global a
a = 3^11*A(1, 1)+3^10*A(1, 2)+3^9*A(2, 1)+3^8*A(2, 2)+
       3^7*B(1, 1)+3^6*B(1, 2)+3^5*B(2, 1)+3^4*B(2, 2)+
         3^3*C(1, 1)+3^2*C(1, 2)+3*C(2, 1)+C(2, 2);

x = [1:3^12 - 1];
global x

global x
for i = 1:6560   x(i) = 0; end
```

```
global A;
global B;
global C;
global M;
global N;
global a;
for i = 6560:3^12 - 1
  jo(i);
    if A == zeros(2)  x(i) = 0;
      if B == zeros(2)  x(i) = 0;
       if C == zeros(2)  x(i) = 0;
         if rem( (A + B), 3) == 0 x(i) = 0;
         if rem( (A + C), 3) == 0 x(i) = 0;
       if rem( (B + C), 3) == 0 x(i) = 0;
      if rem( (A + 2*B), 3) == 0 x(i) = 0;
    if rem( (A + 2*C), 3) == 0 x(i) = 0;
  if rem( (B + 2*C), 3) == 0 x(i) = 0;
if rem( (A + B + C), 3) == 0 x(i) = 0;
  if rem( (A + B + 2*C), 3) == 0 x(i) = 0;
    if rem( (A + 2*B + C), 3) == 0 x(i) = 0;
      if rem( (A + 2*B + 2*C), 3) == 0 x(i) = 0;
      end
    end
  end
end
  end
   end
    end
      end
       end
       end
      end
     end
   end
end
for k = 6561:3^12 - 1
 if x(k) ~= 0
  jo(k);
    for i = 1:80
      joh(i);
        if rem( det(M), 3) ~= 0
          for j = 1:19682
            john(j);
              if rem( det(N), 3) ~= 0
                X = M * A * M';
                Y = M * B * M';
                Z = M * C * M';
                F = N(1, 1)*X + N(1, 2)*Y + N(1, 3)*Z;
                G = N(2, 1)*X + N(2, 2)*Y + N(2, 3)*Z;
                H = N(3, 1)*X + N(3, 2)*Y + N(3, 3)*Z;
                J = rem(F, 3);
```

```
                K = rem(G, 3);
                L = rem(H, 3);
                ph(J, K, L);
                if a ~= k  x(i) = 0;
                end
              end
           end
         end
     end
  end
end

global x;
n = 0;
  for i = 6561:3^12 - 1
    if  x(i) ~= 0
      n = n + 1;
       jo(i)
       A
       B
       C
     end
  end
n
```